CLAIMS

The present listing of claims replaces all the previous versions or listings of the claims:

1. (Currently Amended) A system for real-time vulnerability assessment of a host/device, said system comprising:

an agent running on the host/device, said agent comprising~~:~~

~~a first data structure for storing the status of interfaces and ports on the interfaces of the host/device,~~

an executable agent module ~~coupled to the first data structure~~ configured to track the status of interfaces and ports on the interfaces of the host/device and to store the information[,] as information entries ~~in said first data structure~~,

said executable agent module configured to compare the entries to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device,

a remote destination server~~, said destination server~~ comprising~~:~~

~~a second data structure for storing the status of interfaces and the ports on the interfaces of the host/device,~~

an executable server module ~~coupled to the second data structure~~ configured to receive the information entries communicated by the ~~agent~~ executable agent module ~~of the agent on the host/device~~,

said executable server module configured to store the received information entries, ~~as entries in the second data structure~~ wherein the information entries indicate the state of each of the ports on each of the active interfaces of the host/device ~~as received~~,

said executable server module configured to compare the received information entries ~~in said data structures~~ to determine the change in the status of interfaces and ports on the interfaces of the host/device, and

said executable server module configured to run vulnerability assessment tests on the host/device in the event of a change in the status of interface/ports.

2. (Currently Amended) The system of claim 1~~, further comprising~~: wherein said ~~an~~ executable server module is configured ~~coupled to a second data structure~~ to receive and update the vulnerability data in a vulnerability database ~~the destination server used by the server for vulnerability tests,~~ whenever new vulnerabilities are discovered, and wherein said executable server module is configured ~~coupled to the second data structure~~ to test the host/device for the new vulnerabilities whenever the vulnerability database is updated with new vulnerabilities, and to determine the new vulnerabilities.

3. (Currently Amended) A system for real-time vulnerability assessment of a host/device, said system comprising:

an agent running on the host/device, said agent comprising:

~~a first data structure to store the status of interfaces on the host/device and the ports on the interfaces on the host/device,~~

an executable agent module ~~coupled to the first data structure and operable~~ configured to track the status of interfaces and ports on the interfaces of the host/device to collect and store the information[,] as information entries ~~in the first data structure~~,

said executable agent module ~~coupled~~ configured to ~~the first data structure to~~ compare the entries to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device,

wherein said executable agent module is configured to communicate said changes to a remotely located destination server on ~~the~~ a network, and

a destination server running remotely, said destination server communicably coupled to the host/device over a network, said destination server comprising:

~~a second data structure for storing the status of interfaces/ports on the host/device,~~

an executable server module ~~coupled to the second data structure~~ configured to receive information entries communicated by the executable agent module on the host/device,

said executable server module ~~coupled to the second data structure~~ confiured to store the received information entries, ~~as entries in the second data structure~~ wherein the information entries indicate the state of each of the ports on each of the active interfaces of the host/device ~~as received~~,

said executable server module ~~coupled to the second data structure~~ configured to compare the received information entries to determine any change in the status of interfaces and ports on the interfaces of the host/device ~~as reported to it~~,

said executable server module ~~coupled to the second data structure~~ configured to process the changes to determine any new interfaces active and/or any newly opened ports on any of the active interfaces on the host/device on which services are listening as reported to ~~it~~ said destination server,

said executable server module ~~coupled to the second data structure~~ configured to run tests remotely to identify the network services running on the newly opened ports on the various active interfaces of the host/device,

said executable server module ~~coupled to the second data structure~~ configured to run vulnerability assessment tests on the identified network services on the newly opened ports of the interfaces and storing the results, and

said executable server module ~~coupled to the second data structure~~ configured to obtain an incremental or an overall vulnerability status report of the host/device from the results of the current vulnerability tests, and previously stored vulnerability test results.

4. (Currently Amended) The system of claim 3~~, further comprising:~~ wherein

~~an~~ said executable server module ~~coupled to the second data structure~~ is configured to receive and update the vulnerability database in ~~the~~ a vulnerability assessment server used by the destination server to do vulnerability tests, whenever new vulnerabilities are discovered publicly or elsewhere, and

~~an~~ wherein said executable server module ~~coupled to the second data structure~~ is configured to test the host/device for the new vulnerabilities whenever the vulnerability database is updated with new vulnerabilities, and obtain results.

5. (Previously Presented) The system of claims 1 or 4, wherein status of an interface is either active or inactive.

6. (Previously Presented) The system of claims 1 or 4, wherein status of a port is a service listening on the port or not.

7. (Previously Presented) The system of claims 1 or 4, wherein the agent tracks the change in status of ports/interface by monitoring in real-time or polling at periodic intervals for the status of ports/interfaces and storing the entries at various time intervals.

8. (Previously Presented) The system of claims 1 or 4, wherein the communication protocol between the host/device and the destination server is a standard transport level utility selected from sockets or any other standard communication protocol.

9. (Previously Presented) The system of claims 1 or 4, wherein the server executable module compares the entries corresponding two consecutive time intervals.

10. (Previously Presented) The system of claims 1 or 4, wherein the host/device is selected from a switch, a router, a device running a standard real-time operating system, a mobile device or a PDA.

11. (Previously Presented) The system of claims 1 or 4, wherein the host/device is an enterprise/consumer machine running with Windows, Unix, Linux, VxWorks, Symbian or PalmOS.

12. (Previously Presented) The system of claims 1 or 4, wherein the changes that are communicated to the destination server consisting of the IP address of the interface(s) and the port numbers on which listening services have started or stopped on the particular interface(s).

13. (Previously Presented) The system of claims 1 or 4, wherein the status of the port consists of separate statuses for TC and UD protocols.

14. (Previously Presented) The system of claims 1 or 4, wherein plurality of hosts/devices is tracked in conjunction with one or more destination servers handling the host/devices.

15. (Previously Presented) Logic encoded in a program stored in a computer-readable media for real-time vulnerability assessment of a host/device, and operable to perform the following steps:

tracking in real-time the status of interfaces and/or of the ports on a host/device,

communicating a change in the status of the interfaces and/or the status of ports of the host/device to a remotely located destination server on the network,

tracking in real-time the reported status of ports and interfaces of the host/device by the destination server, and

conducting vulnerability assessment tests on the host/device by the destination server in the event of a change in the status of interfaces and/or ports of the host/device.

16. (Previously Presented) Logic encoded in a program stored in a computer-readable media for real-time vulnerability assessment of a host/device, and operable to perform the following steps:

tracking in real-time the status of interfaces and/or ports on a host/device,

communicating the change in the status of the interfaces and/or the status of ports to a remotely located destination server on the network,

tracking in real-time the reported status of the ports and interfaces of the host/device by the destination server

processing the changes by the destination server to determine new active interfaces or newly opened ports on any of the active interfaces on the host/device on which services are listening,

running tests to identify remotely the network services running on the newly opened ports on the various active interfaces of the host/device,

running vulnerability assessment tests on the identified network services on the newly opened ports of the interfaces and storing the results, and

generating an incremental and/or overall vulnerability status report of the host/device from the results of the current vulnerability tests, and storing the results classified port and interface wise.

17. (Previously Presented) The logic of claims 15 or 16, wherein the status of an interface is either active or inactive.

18. (Previously Presented) The logic of claims 15 or 16, wherein status of a port is a service listening on the port or not.

19. (Previously Presented) The logic of claims 15 or 16, wherein the status of the port consists of separate statuses for TC and UD protocols.

20. (Previously Presented) The logic of claims 15 or 16, wherein tracking consists of monitoring in real-time or polling at periodic intervals for the status of ports/interfaces on the host/device.

21. (Previously Presented) The logic of claims 15 or 16, wherein the communication protocol between the host/device and the destination server is a standard transport level utility selected from sockets or any other standard communication protocol.

22. (Previously Presented) The logic of claims 15 or 16, wherein the host/device is selected from a switch, a router, a device running a standard real-time operating system, a mobile device or a PDA.

23. (Previously Presented) The logic of claims 15 or 16, wherein the host/device is an enterprise/consumer machine running with Windows, Unix, Linux, VxWorks Symbian or PalmOS.

24. (Previously Presented) The logic of claims 15 or 16, wherein the changes that are communicated to the destination server consisting of the IP address of the interface(s) and the port numbers on which listening services have started or stopped on the particular interface(s).

25. (Previously Presented) The logic of claims 15 or 16, wherein the information that is communicated from the host/device to the destination server is the names of the services.

26. (Previously Presented) The logic of claims 15 or 16, wherein the information that is communicated from the host/device to the destination server is a message signaling a change in the status of interfaces and/or ports on the host/device.

27. (Previously Presented) The logic of claims 15 or 16, wherein the vulnerability assessment server used by the destination server is updated with the new vulnerabilities to test the presence of vulnerabilities.

28. (Previously Presented) The logic of claims 15 or 16, wherein a plurality of hosts/devices are tracked in conjunction with plurality of destination servers handling the host/devices.

29. (Currently amended) A computer-implemented method for real-time vulnerability assessment of a host/device, said method comprising:

tracking in real-time the status of interfaces and ports on the host/device[,];

collecting and storing the status as information entries ~~in a data structure~~[,];

comparing the entries to determine any change in the status of interfaces and/or the status of ports on the interfaces of the host/device[,];

communicating the changes to a remotely located destination server on the network[,];

storing said changes as entries in ~~a data structure by~~ the destination server wherein the entries indicate the state of each of the ports on each of the active interfaces of the host/device as reported[,];

comparing the entries ~~by~~ stored at the destination server to determine if there is any change in the status of interfaces and ports on the interfaces of the host/device as reported to it[,]; and

running vulnerability assessment tests on the host/device by the destination server and reporting the results.

30. (Previously Presented) A computer-implemented method for real-time vulnerability assessment of a host/device, said method comprising: polling the status of the ports and interfaces on the host/device, periodically at a pre-configured time interval,

collecting the above information and storing as entries in an agent,

comparing the entries to determine if there is any change in the status of interfaces and/or the status of ports on the interfaces of the host/device,

communicating the changes to a remotely located destination server on the network,

storing the received information as entries in a server by the destination server wherein the entries indicate the state of each of the ports on each of the active interfaces of the host/device as reported,

comparing the entries by the destination server to determine if there is any change in the status of interfaces and ports on the interfaces of the host/device as reported to it, and

running vulnerability assessment tests on the host/device by the destination server and reporting the results.

31. (Previously Presented) The method of claims 29 or 30, wherein the status of an interface is either active or inactive.

32. (Previously Presented) The method of claim 29 or 30, wherein the status of a port is a service listening on the port or not.

33. (Previously Presented) The method of claim 29 or 30, wherein the agent tracks the change in status of ports/interface by monitoring in real-time or polling at periodic intervals for the status of ports/interfaces and storing the entries at various time intervals.

34. (Previously Presented) The method of claim 29 or 30, wherein the communication protocol between the host/device and the destination server is a standard transport level utility selected from sockets or any other standard communication protocol.

35. (Previously Presented) The method of claim 29 or 30, wherein the server executable module compares the entries corresponding two consecutive time intervals.

36. (Previously Presented) The method of claim 29 or 30, wherein the changes that are communicated to the destination server consisting of the IP address of the interface(s) and the port numbers on which listening services have started or stopped on the particular interface(s).

37. (Previously Presented) The method of claim 29 or 30, wherein the status of the port consists of separate statuses for TC and UD protocols.

38. (Previously Presented) The method of claim 29 or 30, wherein plurality of hosts/devices is tracked in conjunction with one or more destination servers handling the host/devices.